Checklist Program Overview

Tim Grance
Thursday, September 25, 2003

NIST Panel Organization

- Introduction
  - Laws, purpose and scope of panel
- What is a Checklist
  - Overview of checklists
- Checklist Lifecycle
  - From submission to publication to maintenance and updates

Organization (cont.)

- Checklist Development Process
  - NIST proposed process
- Incentives for developing checklist
  - What business benefits are there to developing a checklist
- Templates for Checklists

Introduction

- The Cyber Security Research and Development Act of 2002 tasked NIST to develop a checklist setting forth settings that minimize the security risks to Federal government computer systems.
- To fulfill this requirement NIST has developed a method where by outside contributors can voluntarily submit checklists to NIST for publication

Authority

- The Federal Information Security Management Act (FISMA) of 2002
- NIST tasked with developing standards and guidelines to provide adequate security for government agencies (excluding national security agencies)
- Guidelines are consistent with Office of Management and Budget (OMB) requirements for Securing Agency Information Systems

Purpose and Scope of Checklist Guidelines

- Define the procedures and templates for checklist producers to submit those checklists and related information to NIST
- These standard templates will provide a way to allow checklists to be cataloged and searchable
- Provide for a method (i.e. the Web Portal) of easily querying for a specific checklist or multiple checklists.

Panel Overview

- What a checklist is and why it is important
- The Web Portal to access checklists
- How checklists are developed
- NIST's proposed development methodology
  - Threat analysis
  - Environment Definition
  - Testing and quality assurance
- Checklist Lifecycle
- Submission incentives

What is a security checklist?

- Framework for secure settings and deployment
- Checklists also encompass hardening documents, lock down procedures and other tools to secure IT products
- Should be implemented by all users and organizations regardless of size or expertise

Who can benefit from a Security Checklist

- Among the groups that can benefit from a security checklist are:
  - Home Users
  - IT product purchasers
  - System Administrators
  - IT Security Officers
  - IT Security Auditors
  - Security Instructors

Why use a Security Checklist

- The current networked environment is one of constant threat. Parties are constantly searching the network for vulnerable machines to exploit. (e.g. the recent MS Blaster exploit)
- Vulnerable hosts can not only be exploited but also be used to attack and exploit other machines.
- Most default configurations are insecure.
- Very cost effective way to implement industry recommended security practices regardless of organizational size (from home user to large enterprise).

What are the benefits of a Security Checklist

- Among the many benefits of a Security checklist are:
  - To protect systems from both external and internal threats and malicious behavior.
  - To create a hardened environment that reduces the threat of future vulnerabilities such as hidden flaws or bugs inherent in software implementation or weaknesses in protocol
  - To significantly reduce the time required to research and develop appropriate security configurations for installed IT products.
  - To allow smaller organizations or individuals to leverage outside resources to implement recommended practice security configurations

Where to use a Security Checklist

- All environments ranging from the home to a geographically diverse high risk organizations are appropriate places to use a security checklist
- To assist with layered defense initiatives
- To assist in securing potential security exposures introduced remote connections into the enterprise network (e.g. VPN users)

How can NIST help?

- Central repository for security checklists
- Public web portal for quick, efficient, searchable access to the checklists
- Provide information to compare and evaluate published checklists

Checklist Portal and Usage

John Wack
Thursday, September 25, 2003

Information Technology Laboratory
Computer Security Division
NIST National Institute of Standards and Technology

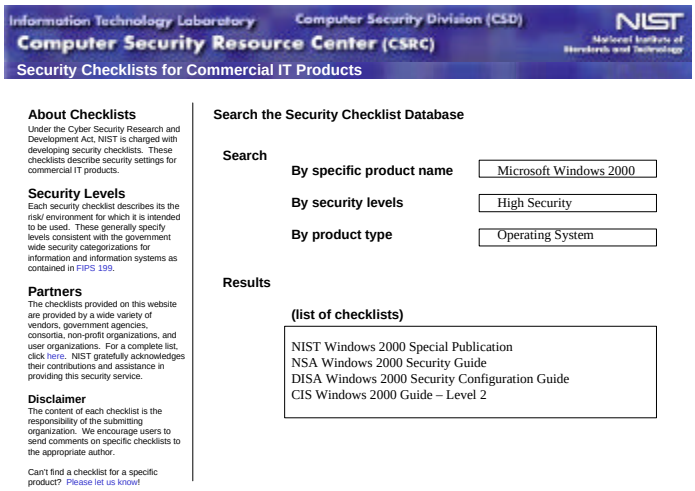
Web Portal Usage

- Checklist users can use a web portal for the following:
  - To locate a checklist for their product
  - To make a purchasing choice based in part on whether a checklist exists
  - To research best practices
- Users include system admins, auditors, trainers, consortia, home users, etc.

Checklist Feedback

- The web portal will permit feedback to checklist submitters.
- Submitters will need to respond within TBD time to questions.
- Exceptions may include proprietary checklists.

Sample Checklist Portal



Using a Checklist

- This will depend on the organization and environment, e.g., home usage vs. large corporation.
- Various checklist template criteria are used to determine whether the checklist is appropriate for your environment:
  - System role
  - Testing procedure
  - Target environment
  - Target audience
  - Prerequisite
  - Known Issues
  - Current Usage

Deploying a Checklist

- Could be deployed directly, but may likely involve local policy modifications.
- Checklists could be designed to anticipate these tradeoffs.
- E.g., a firewall checklist may recommend disabling inbound ICMP packets for an enterprise target environment.
- This could be flagged to be a policy-dependent setting, as effect will block ability to ping.
- Checklists should identify alternatives for enhanced security.

Basic Development Methodology

Tony Harris
Murugiah Souppaya
Thursday, September 25, 2003

Checklist Producers

- IT vendors
- Consortia
- Industry
- Government
- others in public and private sectors

Development Methodology

Product Threat Analysis

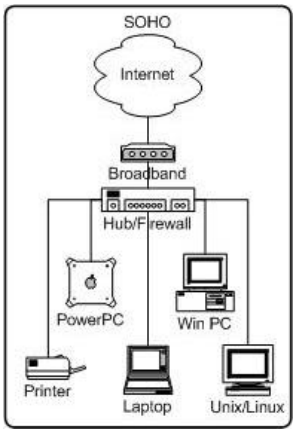
- Requires deep IT Product knowledge
- Vulnerability Analysis
  - Identify vulnerabilities
  - Create mitigation strategy
  - Identify configuration settings to apply recommended practice security settings

Define the Environment

- 3 specific environments
  - SOHO
  - Enterprise
  - High Security
- 1 custom environment

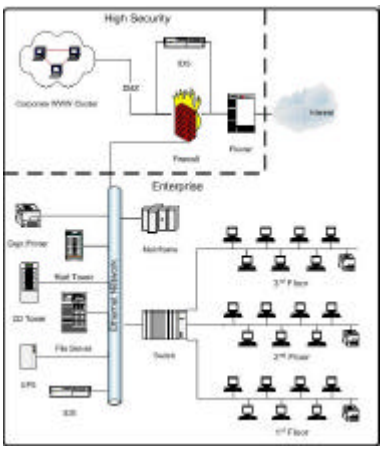
SOHO

- Least functionally restrictive
- Meets basic requirements for common out of the box vulnerabilities
- Home users, Small business



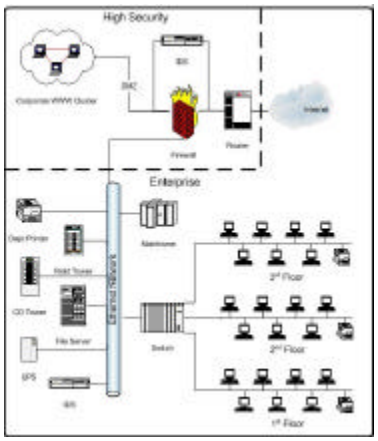
Enterprise

- Centralized
- Managed
- Large Corporate
- Government
- User access restricted



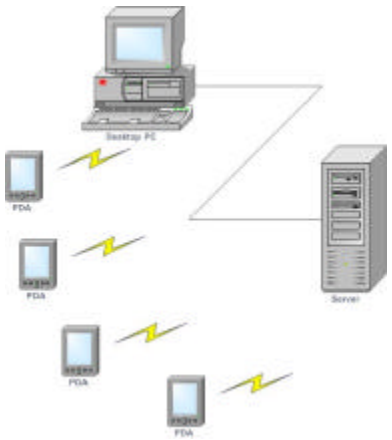
High Security

- Most restricted
- Managed
- No user physical access
- Publicly accessible service
- Standalone possible
- Single purpose

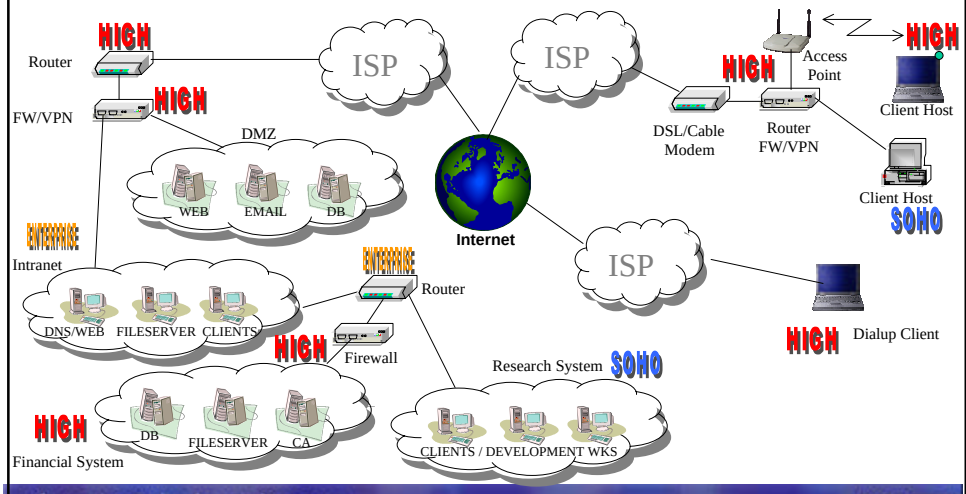


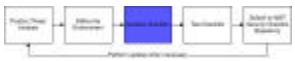
Custom

- Does not fit into other levels
- Not feasible to fully secure product
- Not cost effective
- Acceptable risk



Deployed Environment





Develop Checklist

- Create Checklist based on Vulnerability analysis and target environment
- Usable and reasonable configuration for the target environment
- executable, document, inf, bat, ASCII text, rpm, excel spreadsheet, Web page

Checklist Testing

Arnold Johnson

Thursday, September 25, 2003

Evaluation/Testing/ Assurance

- Some possible approaches
- Only a list for consideration – should not be viewed as a recommendation
- Need to consider impact of cost and effort when requiring any approach

Evaluation / Testing Sources

- 1st Party – Developer
- 2nd Party – Consumer
- 3rd Party – Independent
- Combination

What can be Evaluated

- Documents / Specifications
  - **Completeness**: all parts have been covered; all relevant information provided
  - **Consistent**: doesn't contradict other elements within the document, or has no apparent contradiction with external entities
  - **Coherent**: logically order; understandable by target audience

What can be Evaluated / Tested

- Implementation
  - **Supports stated security policies, objectives and profile**
  - **Product features used**
  - **Implementation parameters selected**
  - **Environments applicable**

Evidence

- Evaluation / testing methodology
- Evaluation / test reports
- Physical evidence to support evaluation / test results

Other Assurances

- Supplier commitment to maintenance / support / configuration control
- Supplier declaration to ensure correct implementation of product functions
- Supplier assurances of applicability to derived environments
- Consumer objective reports of experiences in applying checklists

Checklist Template Framework

Tony Harris
Murugiah Souppaya
Thursday, September 25, 2003

Information Technology Laboratory
Computer Security Division
NIST National Institute of Standards and Technology

Why use a Template?

- Classify, order, and sort the security checklists
- Need for 'standard template' for construction of checklists
  - Usability
  - Searchability
- Search the database based on the fields
- Consistent database entries
  - Standard defined fields (following slides)

Security Template Fields - 1

1. **Manufacturer Name,** *i.e. Microsoft.*
2. **Product category,** *i.e. Client Operating System*
3. **Product Name,** *i.e. Windows 2000 Professional*
4. **Product Version,** *i.e. Service Pack 3*
5. **Checklist Name,** *i.e NIST System Administration Guidance for Windows 2000 Professional Document*
6. **Submitting organization/authors,** *i.e. NIST Computer Security Division*
7. **Checklist creation Date**, *i.e. November 2002*
8. **Latest rev Date,** *i.e. November 2002*

Security Template Fields - 2

8. Target environment, *i.e. Managed environment corporate network protected by border routers and firewalls*
9. Target audience, *i.e. Security Specialists*
10. System role, *i.e. Client desktop host*
11. Firmware/software patch levels, *i.e. MS03-008*
12. Prerequisite, *i.e. familiar with active directory, group policy, etc.*
13. Tools, *i.e. HFNetChk 3.86, Security Configuration Analysis, Secedit, etc.*

Security Template Fields - 3

14. Checklist guide, *i.e. NIST System Administration guidance for Windows 2000 Professional*
15. Checklist Configuration file, *i.e. win2kpro_consensus.inf*
16. Checklist Configuration File Summary, *i.e. table summarizing the recommended parameters*
17. Assessment, *i.e. CIS Scoring tool, MBSA, Nessus, etc.*
18. Known issues, *i.e. Null session, LanMan, IIS, etc.*
19. Checklist Version, *i.e. Version 1.1*
20. Change history, *i.e. Version 1.1*

Security Template Fields - 4

21. Current Usage, *i.e. NIST*
22. Testing Model, *i.e. second party testing*
23. Testing Procedures, *i.e. Detailed in Test Report*
24. Point of contact, *i.e. itsec@nist.gov*
25. References, *i.e. Microsoft Windows 2000 Security Guide, NSA Windows 2000 Guidance, DISA Windows 2000 Guidance, CIS Windows 2000 level benchmark, etc.*
26. References to published vulnerabilities, *i.e. ICAT*

Security Template Fields - 5

21. Roll-back capability, *i.e. no*
22. Vendor Support, *i.e. yes*
23. NIAP/CMVP evaluated, *i.e. no*
24. Comments, Warnings, Disclaimer, Miscellaneous, *i.e. Any additional info the producer would like to relay to the consumer.*

Checklist Lifecycle, Submission, and Incentives

John Wack
Thursday, September 25, 2003

Checklist Lifecycle

- Submitter downloads an RTF template and completes all fields.
- NIST reviews for consistency and, if possible, limited technical content.
- NIST publicizes new checklist through announcements.
- NIST forwards and facilitates feedback for submitter.

Submission to NIST Website

- In order to submit a checklist to NIST, various criteria must be met via the checklist template fields.
- NIST will work with the submitter and review/post the checklist within a reasonable, e.g., two week timeframe.
- Vendor may wish to apply to use a checklist logo after checklist is accepted and posted.

Checklist Logo

- Logo and phrase could be used on promotional materials to show that a product has an associated checklist available.
- Vendor would need to agree to certain conditions on use.

Example Conditions

- NIST reserves the right to control the quality of the use of the logo.
- Vendor agrees to follow the checklist format as described in *NIST Special Publication XX, NIST IT Products Security Template Usage Guidelines, September, 2003.*
- The logo must be used only in conjunction with products that are listed on the NIST checklist portal, http://csrc.nist.gov/checklists.
- The usage of the logo must include the checklist version as listed on the NIST checklist portal.
- Vendor agrees to answer questions regarding checklist usage via industry standard methods, e.g., a dedicated email address, web site, or telephone number. Questions must be addressed within a timely manner.
- Vendor agrees to test the checklist according to the procedures in *NIST Special Publication XX, NIST IT Products Security Template Usage Guidelines, September, 2003.*
- Vendor must issue a modification to the checklist or a new checklist before using the logo on a modified or updated checklist or product.
- NIST retains exclusive rights to the use of the logo; NIST reserves the right to control the quality of the use of the logo.
- Permission for use of the logo may be revoked at the discretion of NIST.
- Permission to use the logo in no way constitutes or implies product or checklist endorsement by NIST.

Questions/Discussion